

In The Boxing Ring



IN THIS ISSUE

2. NETWORK BOX OFFICE CUSTOMER PORTAL

The system enables clients to manage one or more Network Boxes at the country, regional and global levels. It is scheduled to go live this month.

2. PC3 PLATINUM BRAND AWARDS 2008

We have been awarded the Platinum Brand Award in the UTM category.

3. ENCRYPTED SMTP MAIL

If you are concerned about the privacy of your communications you should investigate using encrypted SMTP or a client-side solution.

3. NETWORK BOX INTRUSION AND PREVENTION SYSTEM

We are in the final stages of the development of a new approach to the problem of Intrusion Detection and Prevention.

4. MAY 2009 FEATURES

The ongoing deployment of our recently released features.

Network Box Technical News from Mark Webb-Johnson, CTO Network Box

Welcome

Welcome to the May 2009 edition of 'In the Boxing Ring'. In this edition, the top story is about the Network Box Office Customer Portal. Its key functionality enables users to manage one or more Network Boxes at the country, regional and global levels. The system is scheduled to go live during the first two weeks of May. Details on page 2.

In the latter half of April 2009, Network Box was awarded the PC3 Platinum Brand Award in the UTM category, which included some large global brand names. Turn to page 2 for details.

On page 3, I'll be providing information on Network Box support for SMTPS and STARTTLS and on encrypted SMTP mail – the latter of which I would recommend all our customers look into, if you have yet to do so.

I will also be introducing you to our new approach to the problem of intrusion

detection and prevention – four solutions and when to expect a full release.

And we again have a very large number of significant enhancements for NBR3-3.0 this month. We also have minor changes to the my.network-box.com administrative interface used to query, report on and control a Network Box appliance.

As usual, if you have any feedback, or comments, it is always appreciated. You can contact us here at HQ via email (nbhq@network-box.com). Or, drop by our office next time you are in town.

You can also keep in touch by following our new Network Box Security Response twitter feed at:

twitter.com/networkboxhq

Mark Webb-Johnson

CTO, Network Box Corporation

May 2009





Network Box Office Customer Portal

While our customers' organisational structures may be centralised, distributed or individualised (and any combination of the three), Network Box has always been concerned with the global view.

Our support offices and Network Operations Centres are geographically distributed around the world; but all provide feedback to a centralised system known as Outbreak.

The Network Box Outbreak system currently handles approximately 60,000 security events a minute (about 1,000 each second – more than 86 million a day). A large computer system (nicknamed WOPR) summarises and correlates all those events in real-time. It identifies trends and alerts our security engineers to changes in the global threat landscape.

The Network Box Office Customer Portal gives our customers a window into this (and other) internal systems. It provides real-time status of Network Box devices under our management, and allows for formalised two-way communication with the Network Box Network Operation Centres (NOCs) responsible for monitoring and configuration of the equipment and network. It provides the following key functionality:

- An overview page showing a map of boxes, VPN and management links against a geographic background. This provides a single overview of the managed network. The map is customisable and can show boxes, Internet reachability and VPN links. Pop-up displays allow the user to summarise device status, and hot-links are provided

for connection to other parts of the system.

- A ticketing module showing customer/NOC initiated tickets and their status. This forms the primary communications channel between the customer and the NOC (as it provides for formalised issue tracking, SLA conformance, and authenticated access control to change and configuration requests). This module also includes:
 - A deployment survey module for tracking the information requirements stage of deployments (including gathering the information necessary for deployment, using online collaborative tools).
- An inventory module showing box ownership and status. This module also includes:
 - A health module; interfaced to the Network Box Global Monitoring System (GMS), to show box, gateway and VPN link health status.
- A licensing module; showing contractual agreements (and referenced SLA).
- A workload statistics module; showing box workload and trend analysis.
- A user management module; permitting designated customer administrators to view and maintain Box Office user accounts themselves (without requiring NOC involvement). This module permits the customer greater control and management of the team supporting global deployments.

The system provides a single, simple, powerful web-based user interface for the management of one or more Network Boxes – at the country, regional and global levels.

We are pleased to announce that this system is now scheduled to go live (globally) on 12th May 2009.



PC3 Platinum Brand Awards 2008

Network Box was awarded the platinum brand award for the Unified Threat Management (UMT) category in April 2009.

Nominated under the UTM category of the PC3 Quality Brands Award were Network Box and some of its major competitors.

Being at the forefront of technological development for the defence against growing Internet threats is a tough job, and the competition is fierce. However, while other UTM category nominees are Network Box competitors, all are working towards keeping corporations of all sizes safe from growing digital threats.

Related divisions were Internet Security, including partner Kaspersky, Anti-virus, with nominees NOD32, Trend Micro and others, and Business Security Software, including Sophos, Symantec and other organisations.

Other award groupings included flash memory, IT education, and e-Shop solutions. Further categories focused on Internet security, mobile disks, projector and document solutions.

Overall, there were 45 awards presented with two organisations winning in two categories each. Present were Samsung Electronics, Acronis, Kaspersky, Sony, Asus and many other big-name brands. Sponsors presented the awards in a short, but simple and professional ceremony held at the InnoCentre, Kowloon Tong, Hong Kong.



Encrypted SMTP eMail

As the SMTP standard sends email without using encryption or authentication, every message you send is transmitted in plain text. There are client-side solutions to this (such as S/MIME and PGP). They address the problem very effectively, but require individual user involvement and are complex. A better place to provide fundamental SMTP protection is at the Mail Server / Gateway.

Why would you want to do this? The answer is primarily to avoid the possibility of unwanted eavesdropping on your communications. The real-world equivalent of the SMTP protocol is unsealed letters in the post: your postman, staff at the front door, cleaner, or anyone with physical access to the letter could open and read it, then change and close it again, leaving you none-the-wiser that your "private" communication had been intercepted. If you trust the postman (i.e., the ISPs), or the privacy of your communications is not important, then you need not worry about protecting your

SMTP mail. If you are concerned about this, then you should investigate using encrypted SMTP or one of the client-side solutions (S/MIME or PGP).

Network Box has spent some time adding support for both SMTPS and STARTTLS protocols to both our incoming and outgoing SMTP gateways. The May 2009 patch Tuesday update to our SMTP software will add this support, and we will commence a public beta of the technology in mid/late May (targeting full support during June 2009).

The SMTPS and STARTTLS protocols are built on SMTP and standard SSL/TLS. Thus, they use cryptographic certificates at the server side of the link (and optionally at the client side as well).

Configuring outbound mail to support SMTPS (or STARTTLS) is relatively simple. The Network Box can be configured to operate in 'opportunistic encryption' mode (where it can automatically detect if a server supports STARTTLS and switch to SSL/TLS to encrypt the traffic for all such servers). The Network Box can also be configured to require SMTPS to specified domains or servers.

Configuring inbound mail to support SMTPS (or STARTTLS) requires installing an SSL certificate on the Network Box. These certificates can be purchased online and are fairly simple to obtain. Typically, your purchased certificate would include all the names listed in your published DNS MX records (as the protocol uses these names to authenticate the server is who it says it is). There will normally be a yearly fee.

The Network Box is able to sit in the middle of an encrypted SMTP link. The mail can be encrypted when passed to the Network Box, unencrypted and scanned for malware/spam and company policy enforcement, then re-encrypted as it is passed on to the destination server.

The encrypted SMTP protocols (SMTPS and STARTTLS) are not for everybody. But, they do offer effective support for protecting the SMTP protocol for those who require this protection level. The protocols are standardized and interoperability is excellent.

For further information, please contact your local Network Box support NOC.



Network Box Intrusion Detection & Prevention System

For some time, Network Box has offered an IDP system as part of its managed UTM+ firmware. This is an extremely light-weight, high-speed service, offering zero-latency protection against network worms, exploits and other such attacks.

We are in the final stages of the development of a new approach to the problem of Intrusion Detection & Prevention. This new approach will provide four operation modes (one old, three new):

- Current NBIDS system – lightweight, zero latency, very fast performance.
- New NBIDPS engine, with full stream and protocol disassembly. Able to operate in promiscuous mode (with a switch tap port, or hub), IP-less if required, and in one of three modes:
 - Passive IDS – alerting and logging of traffic, along side the data stream – useful for policy enforcement and more aggressive rules.
 - Active IDS – alerting and logging of traffic, side-by-side with the data stream, but can actively tear-down connections.
 - Inline IPS – alerting and logging of traffic, inline with the data stream; can drop traffic.

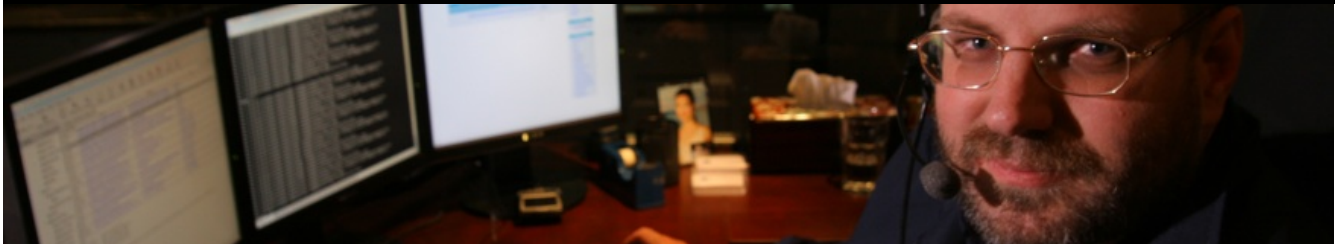
Modes can be combined to suit customer requirements, allowing deployment of the highest possible protection levels, given monetary and performance constraints.

Signatures for the new engine follow the industry-standard Snort format, and can be created on a global, noc, and per-customer basis. An on-the-box system takes the signatures and configurations to produce a live configuration on a per-box basis. Each rule has a documented and retrievable help page for reporting and analysis purposes. We currently have over 10,000 signatures in the new system.

The new engine provides a much more powerful rules language, and more stream and protocol decoders. Good news, but it impacts performance. The solution is to offer the four modes of operation, to balance protection level (and latency) with performance. We can configure different interfaces to operate in different modes (for example, active IDS for LAN policy enforcement, and inline IPS for NET). Or, we can simply operate with one mode for all traffic.

Logging is integrated into our NOC stats/reporting/monitoring systems, as well as periodic reporting and the my.network-box.com administrative functions.

This will be a zero-cost addition to our offering, to all NBRS-3.0 FW+ (or above) clients as part of our ongoing service and monitoring – performance willing. We estimate beta testing will start late May 2009, with a full release during June/July.



May 2009 Features

On Tuesday 5th May 2009, we will be releasing a number of bug fixes and enhancements for NBR3-3.0. These changes include:

- Network Box Office Customer Portal – globally live on 12th May 2009.
- Improvements to the NOC systems for box maintenance, diagnostic and control – including a better centralised auditing system for hybrid NOC / customer configuration changes (such as anti-spam whitelisting/blacklisting).
- New health monitoring checks for DNS servers as well as Google Safe Browsing – to periodically check these systems and alert (via GMS) on problems.
- Support for SMTPS and STARTTLS protocols in our store-and-forward SMTP proxy.
- Support for NBIDPS and periodic reporting on IDPS alerts.
- Some minor changes to the my.network-box.com administrative interface.

The above changes will not require any impacting service or device restarts, and should not cause any significant interruption to device operation. The regional NOCs will be conducting the rollouts of the new functionality in a phased manner.

Should you need any further information on any of the above, please contact your local NOC. They will be arranging deployment and liaison.

May Hint

Network Box has a variety of real-time information feeds available to you, using industry standard protocols and services. I suggest you take advantage of this to get an early insight into what is happening in the world of security and what Network Box is doing for you. To stay informed is to be better prepared.

You can always see top Network Box news stories either on our website, or the home page of my.network-box.com. But, did you know that you can get an RSS feed of this right in your browser / RSS reader? Visit: <http://www.network-box.com/aboutus/news/feed> for our RSS feed.

For even faster cutting-edge news, tips and alerts, follow Security Response at <http://twitter.com/networkboxhq> or <http://tinyurl.com/c49s7v> for an RSS feed.

Conclusions

Thank you for your support of Network Box, and the continued entrustment of your network security to our managed service. I hope you find this communication useful – if you have any suggestions, they are most appreciated, and should be directed towards your local NOC or account manager. Please don't hesitate to contact us for assistance.

Mark Webb-Johnson
 CTO, Network Box Corporation
 May 2009

MAY 2009 NUMBERS

Key Metric)	#	% difference (since last month)
PUSH Updates	1,213	-12.5
Signatures Released	2,083,850	-14.0
Firewall Blocks (/box)	618,154	+8.8
IDP Blocks (/box)	139,060	+12.8
Spams (/box)	35,025	+18.5
Malware (/box)	1,340	+63.2
URL Blocks (/box)	59,193	+9.8
URL Visits (/box)	2,611,502	+3.0

NEWSLETTER STAFF

Mark Webb-Johnson
 Editor

Pauline Chiu
Michael Gazeley
Jason Law
 Production Support

Network Box Australia
Network Box Hong Kong
Network Box UK
 Contributors

SUBSCRIPTION

Network Box Corporation
nbhq@network-box.com
 or via mail at:

Network Box Corporation
 16th Floor, Metro Loft,
 38 Kwai Hei Street,
 Kwai Chung, Hong Kong

Tel: +852 2736-2078
 Fax: +852 2736-2778

www.network-box.com